REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed September 20, 2007.

In the Office Action, claims 1-8 and 23-20 stand rejected under 35 U.S.C. § 112 and claims 1-30 stand rejected under 35 U.S.C. § 103.

Applicant has amended independent claim 1, 9, 16, and 23 to further clarify embodiments of the invention.

Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Rejection Under 35 U.S.C. § 112

Claims 1-8 and 23-30 stand rejected under 35 U.S.C. § 112, second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In particular, the Examiner remarked that this claim was allegedly in conflict with claims 9 and 16 that recite "creating a secure execution environment in which a plurality of separate virtual machines operate..."

In accordance with the Examiner's suggestion, Applicant has amended independent claim 1 and 23 to be more consistent with independent claims 9 and 16.

Applicant respectfully requests that the Examiner remove this ground for rejection.

Rejection Under 35 U.S.C. § 103

Claims 1-30 stand rejected under 35 U.S.C. § 103(a) as being allegedly obvious over U.S. Patent No. 6,496,847 issued to Bugnion et al. (hereinafter Bugnion) in view of U.S. Patent No. 5,459,869 issued to Spilo (hereinafter Spilo).

Applicant respectfully submits that amended independent claims 1, 9, 16, and 23 are not rendered obvious by the combination of Bugnion and Spilo, either alone, or in combination, as

these references to not teach or suggest the limitations of amended independent claims 1, 9, 16, and 23.

In particular, utilizing independent claim 1 as an example, amended independent claim 1 recites a secure virtual machine monitor (SVMM) that responsive to a command to tear down the secure execution environment from *a non-trusted guest OS* causes *the processor to exit out of the secure execution mode*, *scrubs the protected memory area associated with the trusted guest software*, tears down the secure execution environment, and instructs the *non-trusted guest OS* to resume control of the normal execution mode.

It should be noted that the Examiner relies upon column 8, lines 34-40 of Bugnion for many of Bugnion's alleged teachings. However, this citation of Bugnion relates to a VMM 360 that is co-resident with an existing protected operating system (the host operating system 340). Thus, the operating system of Bugnion is a protected operating system and not *a non-trusted guest OS* as in Applicant's claims. It should be noted that Bugnion further recites that the VMM runs independently of the host operating system and it is in no way an extension of the host operating system, but rather operates with its own address space and with its own interrupt and exception handlers. Bugnion goes on to describe that the virtualization system includes a device emulator 300 that runs as a user-level application on top of the host operating system 340. (See Bugnion column 8, lines 34-40).

Thus, Bugnion teaches a protected host operating system that operates completely independently of the VMM.

As to Spilo, as set forth in the Abstract of Spilo (as relied upon by the Examiner), Spilo generally relates to: A method and system for allowing protected mode device drivers and resident programs to load and execute from an MS/PC-DOS environment...enabling protected mode programs...to transition between host environments...allowing for protected mode programs running in DOS [to] transition and continue to function in Windows environment...[and to] improved method of mode switching for such drivers...

In contrast to both Bugnion and Spilo, Applicant's claim recite a SVMM that responsive to a command to tear down the secure execution environment from *a non-trusted guest OS*

causes the processor to exit out of the secure execution mode. Thus, *a non-trusted guest OS* operates *in conjunction* with the *secure virtual machine monitor (SVMM)*.

Accordingly, both Bugnion and Spilo teach a very different invention than that recited by Applicant's claim and, in fact, Bugnion teaches away from Applicant's claims.

Further, Applicant can find no teaching or suggestion in Bugnion or Spilo of the *scrubbing of the protected memory area associated with the trusted guest software followed by the tearing down of the secure execution environment*. Applicant respectfully requests that the Examiner point to a specific teaching of these limitations.

In view of Applicant's claim amendments, Applicant respectfully submits that Bugnion and Spilo, alone, or in combination, do not teach or suggest the limitations of Applicant's amended independent claim 1, 9, 16, and 23 that generally recite a secure virtual machine monitor (SVMM) that *responsive to a command to tear down* the secure execution environment from a *non-trusted guest OS* causes the processor to exit out of the secure execution mode, *scrub the protected memory area associated with the trusted guest software*, tears down the secure execution environment, and instructs the *non-trusted guest OS* to resume control in the normal execution mode.

For at least these reasons, Applicant respectfully submits that amended independent claim 1, 9, 16, and 23, as well as the claims that depend therefrom, are allowable and should be passed to issuance.

Conclusion

In view of the remarks made above, it is respectfully submitted that pending claims 1-3, 5, 7-11, 13, 15-18, 20, 22-25, 27, 29, and 30 are allowable over the prior art of record. Thus, Applicant respectfully submits that all the pending claims are in condition for allowance, and such action is earnestly solicited at the earliest possible date. The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application. To the extent necessary, a petition for an extension of time under 37 C.F.R. is hereby made. Please charge any shortage in fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 12/20/2007

By_____

Eric T. King
Reg. No. 44,188
Tel.: (714) 557-3800 (Pacific Coast)

Attachments

1279 Oakmead Parkway,
Sunnyvale, CA 94085-4040